Assignment 07

cryptology – b keerthana

AMRUTHESH

241059041

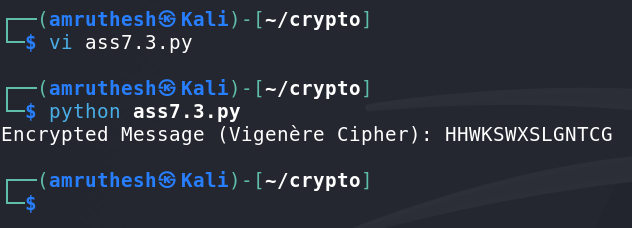
M.E – Cyber Security

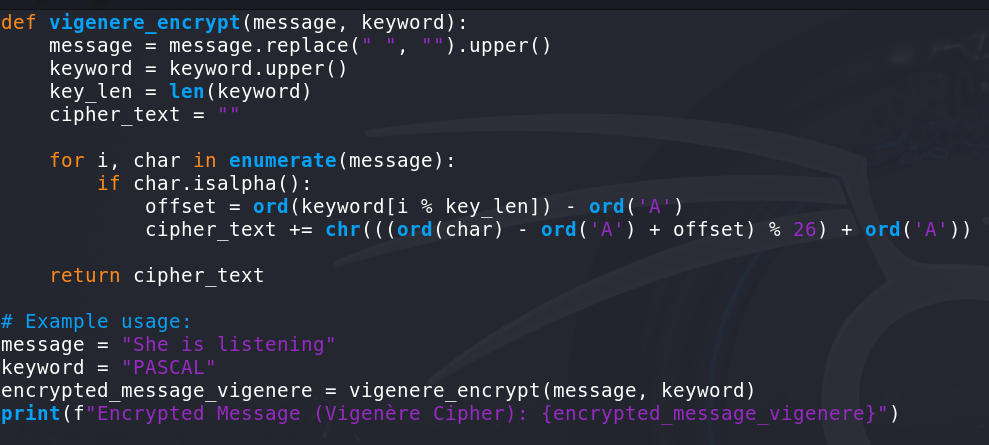
MSIS, MANIPAL

**1. Vigenère Cipher**

The **Vigenère Cipher** is a polyalphabetic substitution cipher that uses a keyword to shift letters in the plaintext. The key is repeated to match the length of the plaintext, and each letter is shifted based on the corresponding letter of the key.

* **Steps**:
  1. Each letter of the plaintext is shifted by the position of the corresponding letter of the keyword.
  2. The keyword is repeated to match the length of the plaintext, and shifts are calculated accordingly.
* **Implementation Details**: In the Python script, the message is first cleaned by removing spaces and converting it to uppercase. The keyword is used to determine the shift for each letter of the message. The shift is calculated by finding the alphabetical position of the key letter and shifting the plaintext letter accordingly. The encrypted message is then returned as the final output.

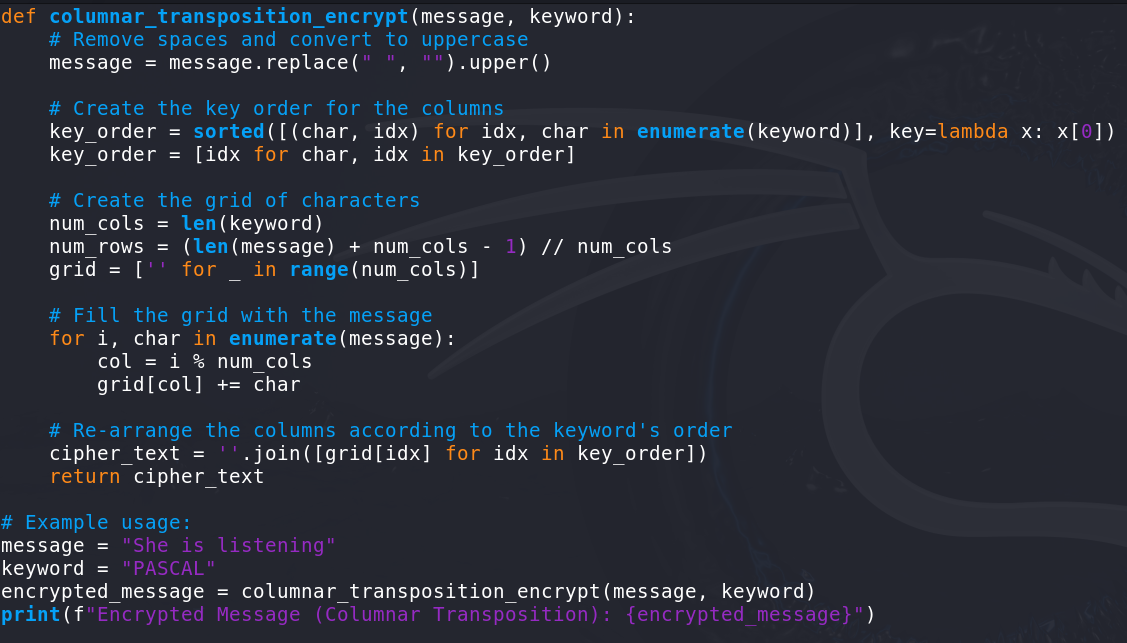


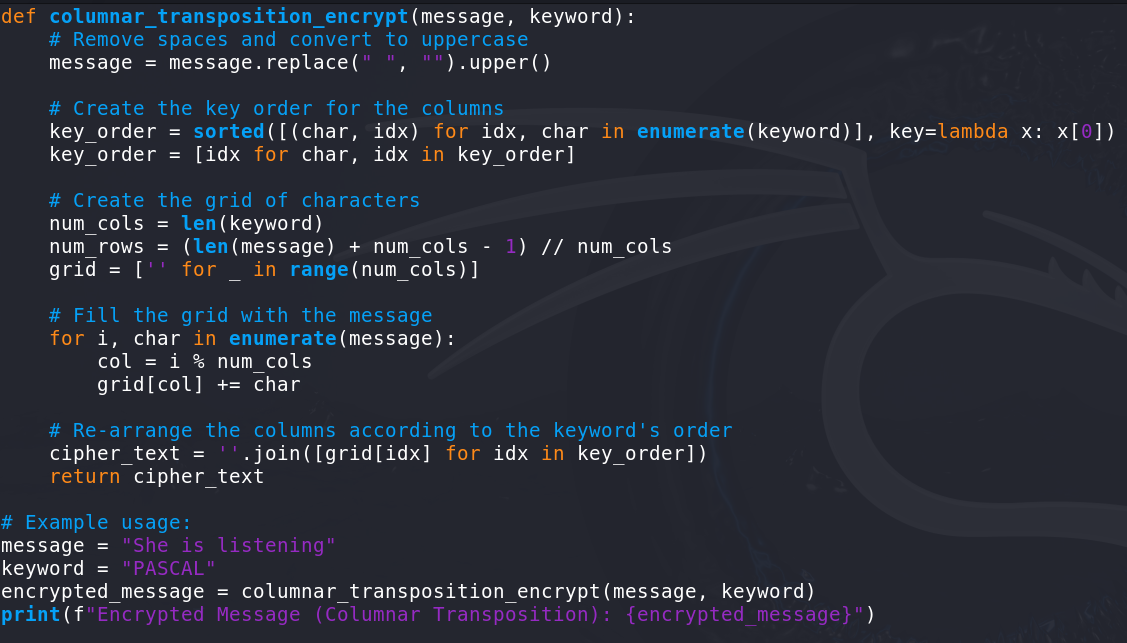


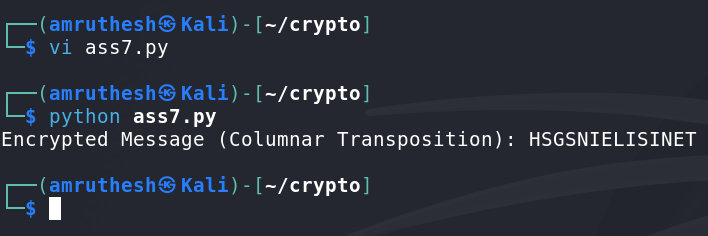
**2. Columnar Transposition Cipher**

The **Columnar Transposition Cipher** is a simple form of transposition cipher where the plaintext is written into rows, and the columns are permuted according to a keyword. The ciphertext is then formed by reading the columns in the order dictated by the keyword.

* **Steps**:
  1. Write the message in rows, with the number of columns equal to the length of the keyword.
  2. Read the columns according to the alphabetical order of the keyword.
* **Implementation Details**: In the Python implementation, the message is first cleaned by removing spaces and converting it to uppercase. The keyword is used to sort the columns in alphabetical order, and then the message is arranged in a grid-like structure. The final ciphertext is constructed by reading the columns in the order determined by the keyword.



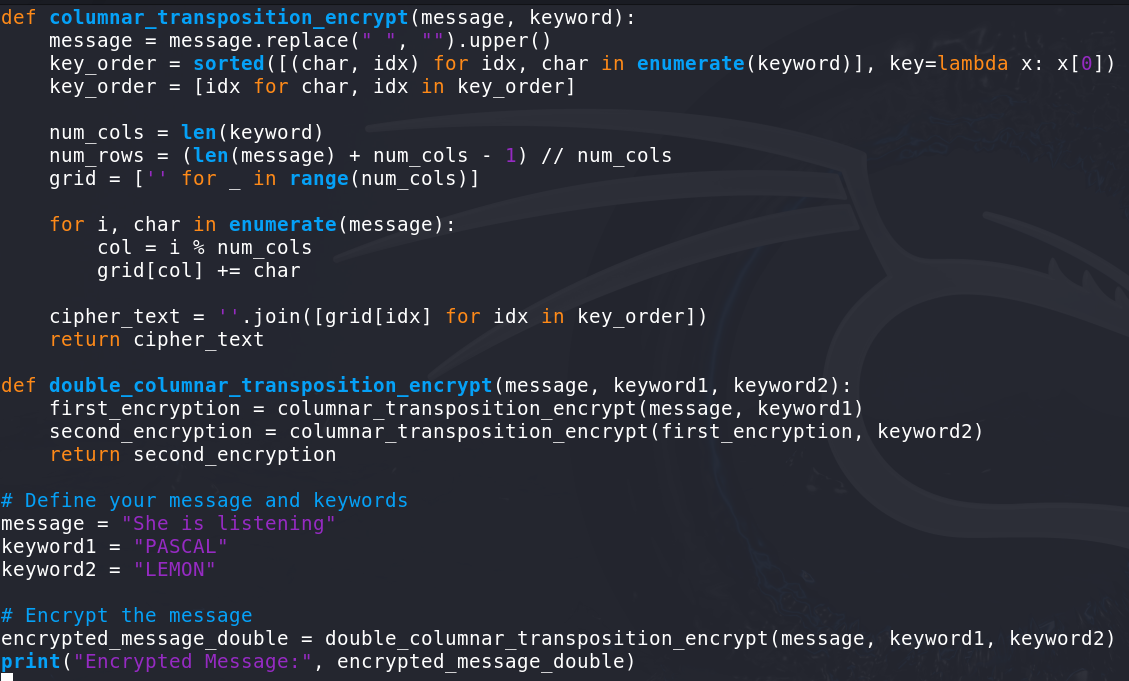
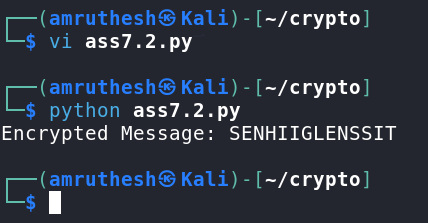




**3. Double Columnar Transposition Cipher**

The **Double Columnar Transposition Cipher** is an extension of the columnar transposition cipher. It applies the columnar transposition cipher twice, each time with a different keyword.

* **Steps**:
  1. Encrypt the plaintext using the first keyword.
  2. Encrypt the result from step 1 using the second keyword.
* **Implementation Details**: The double encryption process ensures that the resulting ciphertext is harder to break. The Python implementation first applies the columnar transposition cipher with the first keyword and then applies it again with a second keyword. This additional layer of encryption enhances security compared to single columnar transposition.



**4. Kasiski Test**

The **Kasiski Test** is a statistical method used to break ciphers, particularly the Vigenère cipher. It helps to determine the key length by analyzing repeated sequences of characters (usually trigrams) in the ciphertext. The distances between these repeated sequences can reveal patterns related to the key length.

* **Steps**:
  1. Search for repeated sequences of three or more characters in the ciphertext.
  2. Calculate the distances between the occurrences of these sequences.
  3. Analyze the most common distances, which often correspond to factors of the key length.
* **Implementation Details**: In the Python script, repeated trigrams in the ciphertext are identified. The distances between their occurrences are calculated, and the most frequent distances are returned. These distances can be analyzed to determine the likely key length.

